

Claims

What is claimed:

1. A computing device, comprising:
a processor;
a memory coupled to the processor; and
program instructions provided to the memory and executable by the processor to:
transmit a network management message over a network to a network device;
collect response information from the network device based on the network management message; and
analyze the response information including applying a Kalman filter to the collected response information.
2. The device of claim 1, wherein the computing device is a network event regulator device.
3. The device of claim 2, wherein the computing device is selected from the group of a wireless access point, a switch, a hub, and a router.
4. The device of claim 1, further including program instructions which execute to regulate external network stimuli based on applying the Kalman filter to reduce degraded performance to the network.
5. The device of claim 1, further including program instructions which execute to signal when abnormal levels of activity are detected based on applying the Kalman filter.
6. The device of claim 1, further including program instructions which execute to track media access control (MAC) layer addressing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network.

7. The device of claim 1, further including program instructions which execute to track internet protocol (IP) flow and routing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network.
8. The device of claim 7, further including program instructions which execute to track IP flow and routing at a network device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router.
9. The device of claim 1, further including program instruction which execute to track information between various network layers in a given protocol stack model and which execute to learn network events based on applying the Kalman filter to the tracked information.
10. The device of claim 9, wherein the various network layers include network layers in a protocol stack model selected from the group of:
- an OSI protocol stack model;
 - an SS7 protocol stack model; and
 - a TCP/IP protocol stack model.
11. The device of claim 9, wherein the various network layers include network layers selected from the group of:
- a TCP port-level connection;
 - a session level connection;
 - a presentation level connection;
 - an application level connection;
 - a transaction capabilities application part level (TCAP) level connection;
 - an integrated services digital network user part (ISUP) level connection;
 - a mobile application part (MAP) level connection; and
 - a signaling connection control point (SCCP) level connection.

12. A computing device, comprising:
a processor;
a memory coupled to the processor; and
program instructions provided to the memory and executable by the processor to:
collect information from a network device connected to the computing device over a network;
analyze collected information including applying a Kalman filter to the collected response information; and
regulate external network stimuli based on applying the Kalman filter to reduce degraded performance on the network.
13. The computing device of claim 12, further including collecting information from the network device selected from the group of:
processor utilization;
memory utilization;
link up/down status;
traps;
buffer utilization;
local area network (LAN) utilization; and
statistics including discards, cyclical redundancy checking (CRC) and frame check sequence (FCS) errors and number of broadcasts.
14. The computing device of claim 12, further including program instructions which execute to automatically calibrate a threshold in the network device used to control a connection rate to the network device.
15. The computing device of claim 14, further including program instructions which execute to convert the network device to perform a different role.

16. The computing device of claim 15, further including program instructions which execute to convert a network database to serve as a network hub.
17. The computing device of claim 15, further including program instructions which execute to convert a network switch to a network hub.
18. The computing device of claim 12, further including program instructions which execute to track media access control (MAC) layer addressing and, based on applying the Kalman filter, execute to reduce false positives and false negatives.
19. The computing device of claim 12, further including program instructions which execute to track internet protocol (IP) flow and routing and, based on applying the Kalman filter, execute to reduce false positives and false negatives.
20. The computing device of claim 12, wherein the network device includes a network device selected from the group of:
- a switch;
 - a hub;
 - a database;
 - a security appliance;
 - a wireless access point device;
 - a network intrusion device; and
 - a router.
21. The computing device of claim 12, wherein the network device and the computing device are connected over a local area network (LAN).
22. The computing device of claim 12, wherein the network device and the computing device are connected over a wireless wide area network (WAN).

23. A method for network and network device management, comprising:
receiving network information associated with a network device; and
analyzing the network information using a Kalman filter.
24. The method of claim 23, wherein the method includes receiving response information to an SNMP message sent to the network device.
25. The method of claim 23, wherein the method includes receiving information contained in a management information base (MIB) of the network device.
26. The method of claim 23, wherein the method includes using a software agent embedded in the network device to receive and analyze the network information.
27. The method of claim 23, wherein the method includes receiving network information associated with a device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router.
28. The method of claim 23, wherein the method includes receiving media access control (MAC) layer addressing information.
29. The method of claim 23, wherein the method includes receiving internet protocol (IP) flow and routing information.
30. The method of claim 23, wherein the method includes:
receiving information communicated between various network layers in a given protocol stack model; and
learning network events based on applying the Kalman filter to the received information.

31. The method of claim 23, wherein the method includes reducing false positives and false negatives based on applying the Kalman filter to received network information
32. The method of claim 23, wherein the method includes regulating external network stimuli based on applying the Kalman filter to received network information.
33. The method of claim 23, wherein the method includes producing an alert signal when abnormal levels of activity are detected based on analyzing the network information using the Kalman filter.
34. A method for network and network device management, comprising:
collecting information associated with a network device;
analyzing the collected information including applying a Kalman filter to the collected information; and
regulating external network stimuli based on applying the Kalman filter in order to reduce network performance degradation.
35. The method of claim 34, wherein the method includes receiving media access control (MAC) layer addressing information and learning network events based on applying the Kalman filter to the MAC layer addressing information.
36. The method of claim 34, wherein the method includes receiving internet protocol (IP) flow and route information and learning network events based on applying the Kalman filter to the IP flow and route information.
37. The method of claim 34, wherein the method includes converting the network device from a first role to a second role based on applying the Kalman filter to the collected information.
38. The method of claim 34, wherein the method includes automatically calibrating a threshold in the network device used to control a connection rate to

the network device based on applying the Kalman filter to the collected information while the network device is in network use.

39. A computer readable medium having instructions for causing a device to perform a method, comprising:

- receiving network information associated with a network device; and
- analyzing the network information using a Kalman filter.

40. The medium of claim 39, wherein the method further includes automatically calibrating a threshold in the network device used to control a connection rate to the network device based on applying the Kalman filter to the network information while the network device is in network use.

41. The medium of claim 39, wherein the method further includes learning media access control (MAC) layer addressing events based on applying the Kalman filter to MAC layer addressing information.

42. The medium of claim 39, wherein the method further includes learning internet protocol (IP) flow and routing events based on applying the Kalman filter to IP flow and route information.

43. The medium of claim 39, wherein the method further includes converting the network device from a first role to a second role based on applying the Kalman filter to received network information.

44. A network device, comprising:

- a processor;

- a memory coupled to the processor;

- means for regulating external network stimuli based on applying a Kalman filter to information associated with the network device.

45. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on the network device.
46. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on another network device connected to the network device over a local area network.
47. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to convert the network device to a different role.
48. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to reduce network performance degradation on the network device.
49. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to reduce network performance degradation on a different network device.